FortiOS™ Handbook

Devices and Client Reputation for FortiOS 5.0

FortiOS™ Handbook Devices and Client Reputation for FortiOS 5.0

May 15, 2013

01-500-122870-20130515

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Contents

Introduction

Welcome and thank you for selecting Fortinet products for your network protection.

This chapter contains the following topics:

Before you begin

Before you begin using this guide, please ensure that:

- You have administrative access to the web-based manager and/or CLI.
- The FortiGate unit is integrated into your network.
- The operation mode has been configured.
- The system time, DNS settings, administrator password, and network interfaces have been configured.
- Firmware, FortiGuard Antivirus and FortiGuard Antispam updates are completed.
- Any third-party software or servers have been configured using their documentation.

While using the instructions in this guide, note that administrators are assumed to be super_admin administrators unless otherwise specified. Some restrictions will apply to other administrators.

How this guide is organized

This FortiOS Handbook chapter contains the following sections:

Managing “bring your own device” describes device monitoring, devices, device groups, and device policies. The administrator can monitor all types of devices and control their access to network resources.

Endpoint Control describes how you can enforce the use of FortiClient Endpoint Control and apply an endpoint profile to users’ devices. Endpoint profiles include real-time antivirus protection, application control, web category filtering, and VPN provisioning.

Vulnerability Scan describes how perform network vulnerability scanning to look for security weaknesses in your servers and workstations.

Client Reputation describes how you can monitor users/clients for online behavior that could increase the risk of attack or infection. This behavior includes use of untrustworthy software and visits to potentially risky web sites. As well, clients’ unsuccessful connection attempts are tracked as a possible indicator of virus or malware infection. Based on the results of this monitoring, you can determine whether adjustments to your security settings or IT policies are needed.

Managing “bring your own device”

FortiOS can control network access for different types of personal mobile devices that your employees bring onto your premises. You can:

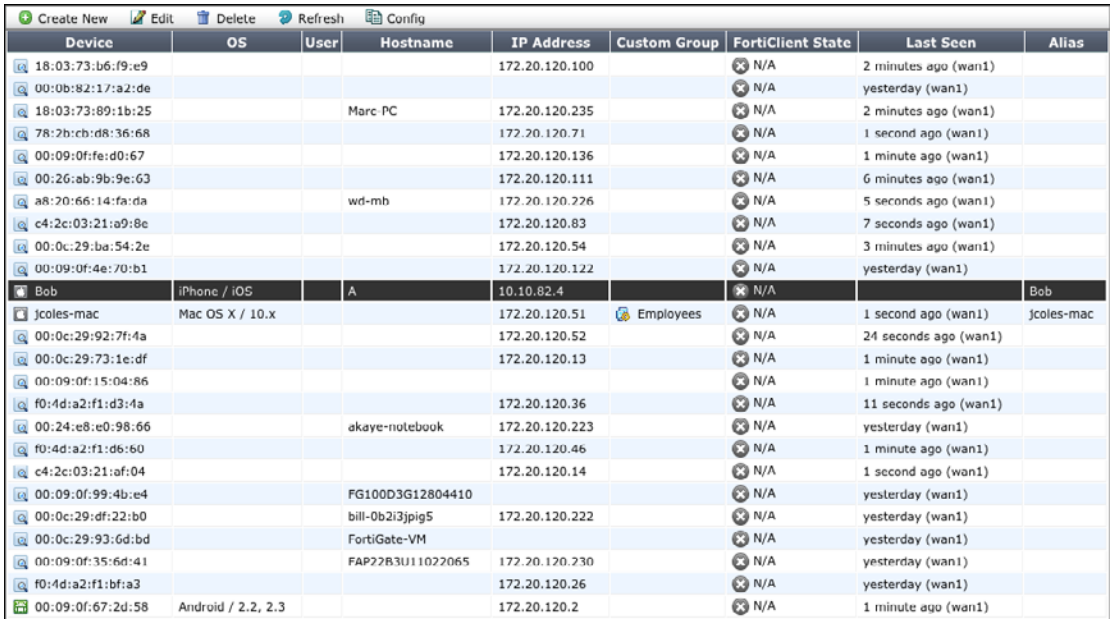
- identify and monitor the types of devices connecting to your networks, wireless or wired
- use MAC address based access control to allow or deny individual devices
- create policies based on device type
- enforce endpoint control on devices that can run FortiClient Endpoint Control software

Device monitoring

The FortiGate unit can monitor your networks and gather information about the devices operating on those networks. Collected information includes:

- MAC address
- IP address
- operating system
- hostname
- user name
- how long ago the device was detected and on which FortiGate interface

You can go to *User & Device* > *Device* > *Device Definition* to view this information.



Device	OS	User	Hostname	IP Address	Custom Group	FortiClient State	Last Seen	Alias
18:03:73:b6:f9:e9				172.20.120.100		N/A	2 minutes ago (wan1)	
00:0b:82:17:a2:de						N/A	yesterday (wan1)	
18:03:73:89:1b:25			Marc PC	172.20.120.235		N/A	2 minutes ago (wan1)	
78:2b:cb:d8:36:68				172.20.120.71		N/A	1 second ago (wan1)	
00:09:0f:fe:d0:67				172.20.120.136		N/A	1 minute ago (wan1)	
00:26:ab:9b:9e:63				172.20.120.111		N/A	6 minutes ago (wan1)	
a8:20:66:14:fa:da			wd-mb	172.20.120.226		N/A	5 seconds ago (wan1)	
c4:2c:03:21:a9:8e				172.20.120.83		N/A	7 seconds ago (wan1)	
00:0c:29:ba:54:2e				172.20.120.54		N/A	3 minutes ago (wan1)	
00:09:0f:4e:70:b1				172.20.120.122		N/A	yesterday (wan1)	
Bob	iPhone / iOS		A	10.10.82.4		N/A		Bob
jcoles-mac	Mac OS X / 10.x			172.20.120.51	Employees	N/A	1 second ago (wan1)	jcoles-mac
00:0c:29:92:7f:4a				172.20.120.52		N/A	24 seconds ago (wan1)	
00:0c:29:73:1e:df				172.20.120.13		N/A	1 minute ago (wan1)	
00:09:0f:15:04:86						N/A	1 minute ago (wan1)	
f0:4d:a2:f1:d3:4a				172.20.120.36		N/A	11 seconds ago (wan1)	
00:24:e8:e0:98:66			akaye-notebook	172.20.120.223		N/A	yesterday (wan1)	
f0:4d:a2:f1:d6:60				172.20.120.46		N/A	1 minute ago (wan1)	
c4:2c:03:21:af:04				172.20.120.14		N/A	1 second ago (wan1)	
00:09:0f:99:4b:e4			FG100D3G12804410			N/A	yesterday (wan1)	
00:0c:29:df:22:b0			bill-0b2i3jpig5	172.20.120.222		N/A	yesterday (wan1)	
00:0c:29:93:6d:bd			FortiGate-VM			N/A	yesterday (wan1)	
00:09:0f:35:6d:41			FAP22B3U11022065	172.20.120.230		N/A	yesterday (wan1)	
f0:4d:a2:f1:bf:a3				172.20.120.26		N/A	yesterday (wan1)	
00:09:0f:67:2d:58	Android / 2.2, 2.3			172.20.120.2		N/A	1 minute ago (wan1)	

Device monitoring is enabled separately on each interface. Device detection is intended for devices directly connected to your LAN ports. If enabled on a WAN port, device detection may be unable to determine some devices’ operating system.

To configure device monitoring

1. Go to *System* > *Network* > *Interface*.
2. Edit the interface that you want to monitor devices on.
3. In *Device Management*, select *Detect and Identify Devices*.
4. Select OK.
5. Repeat steps 2 through 4 for each interface that will monitor devices.

To edit device information

1. Go to *User & Device* > *Device* > *Device Definition* and double-click the entry to edit it.
2. Enter an *Alias* to identify the device.

   This is step is compulsory. The alias replaces the MAC address in the device list.
3. Change other information as needed.
4. Select *OK*.

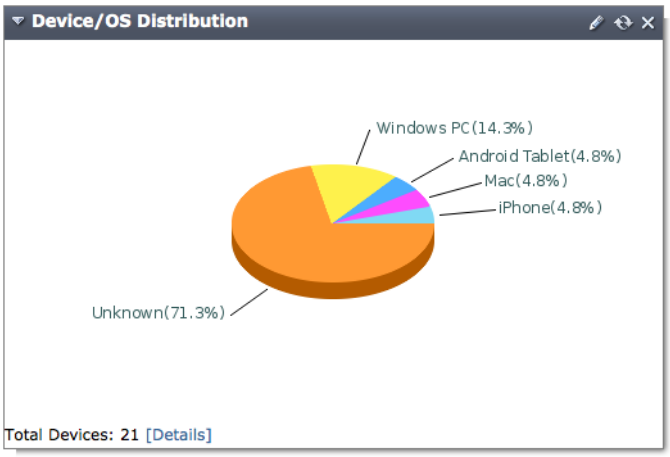
To add a device manually

1. Go to *User & Device* > *Device* > *Device Definition* and select *Create New*.
2. Enter the following information.
   - MAC address
   - Alias (required)
   - Device Type
3. Optionally, select a *Custom Group* or enter *Comments*.
4. Select *OK*.

Viewing device and OS distribution statistics on the dashboard

Device information is summarized on the Dashboard in the Device/OS Distribution widget. The main display is a pie chart that shows the relative numbers of each type of device.

Figure 1: Device/OS Distribution widget display



The Details link displays a table listing the host address, host name, operating system and user name (if known) for each device.

Device Groups

Device Groups are used in device policies to specify which devices match the policy. FortiOS automatically adds detected devices of well-known device types to predefined device groups. You can also create custom device groups so that you can create a different policy for devices that you know than for devices in general.

Go to *User & Device* > *Device* > *Device Group* to view the list of device groups. To view all groups, select *Show Empty Groups* at the top right of the list..

Table 1: Predefined Device Groups

	Devices
Android Phone	All Android-based phones in the Device Visibility database.
Android Tablet	Tablets running Android OS.
BlackBerry Phone	All BlackBerry-based phones in the Device Visibility database.
Collected Emails	All devices from which FortiOS has collected a user email address.
Fortinet Device	FortiGate, FortiManager, FortiAnalyzer, FortiMail, etc.
Gaming Console	All Gaming consoles listed in the Device Visibility database. This includes Xbox, PS2, PS3, Wii, PSP.
iPad	All IOS-based tablets in the Device Visibility database.
iPhone	All IOS-based phones in the Device Visibility database.
IP Phone	All IP phones.
Linux PC	PCs running a Linux-based OS.
Mac	Apple Macintosh computers.
Media Streaming	Media streaming devices such as Apple TV.
Windows Phone	All Windows OS based phones.
Windows PC	PCs running a Windows OS.
Other Network Device	All other network devices not categorized under any other group.
All	All devices.

Creating a custom device group

The predefined device groups are automatically populated. When you create a custom device group, you choose the members. Adding a device that the FortiGate unit has already detected is easiest. But you can also add a device that has not yet been detected if you know its MAC address.

To create the custom device group

1. Go to *User & Device* > *Device* > *Device Group* and select *Create New*.
2. Enter a name, Employees for example.
3. Select *OK*.

To add detected devices to the custom device group

1. Go to *User & Device* > *Device* > *Device Definition*.
2. Right-click the device entry and select *Edit*.
3. Enter an *Alias*, such as the user's name.

   The Alias replaces the MAC address in the device list for easier identification.
4. In *Custom Group*, select the custom group, *Employees*.
5. Select *OK*.
6. Repeat steps 2 through 5 for each additional device.

To add an undetected device to the custom device group

1. Go to *User & Device* > *Device* > *Device* and select *Create New*.
2. Enter the following information.
   - MAC address
   - Alias
   - Device Type
3. In *Custom Group*, select the custom group, *Employees*.
4. Select *OK*.

   The new device is added to the devices list as well as to the custom device group.

Controlling access with a MAC Address Access Control List

A MAC Address Access Control List is best used to handle exceptions. If you want to limit network access to a larger group such as your employees, it is better to create a custom device group and specify that group in your device-based security policies.

A MAC Address Access Control List functions as either a list of blocked devices or a list of allowed devices. This is determined by the *Unknown MAC Address* entry.

- By default, unknown MAC addresses are allowed: *Action* is *Assign IP*. You add an entry for each MAC address that you want to block and set its *Action* to *Block*.
- If you want to restrict access to a limited set of devices, you set the *Unknown MAC Address* entry to *Block* and add an entry for each allowed MAC address with *Action* set to *Assign IP.*

To create a MAC Address Access Control List

1. In the SSID or other interface configuration, select *Enable DHCP Server*.
2. Enter the required *Address Range* and *Netmask*.
3. Expand *MAC Address Access Control List*.
4. Select *Create New* and enter the device's *MAC Address*.
5. Select *Assign IP* to allow the device or *Block* to block the device and then select *OK*.
6. Repeat Steps 4 and 5 for each additional MAC address entry.
7. If needed, edit the *Unknown MAC Address* entry to set the correct *Action*.

Device policies

Policies based on device identity enable you to implement policies according to device type. For example:

- Gaming consoles cannot connect to the company network or the Internet.
- Personal tablet and phone devices can connect to the Internet but not to company servers.
- Company-issued laptop computers can connect to the Internet and company servers. Web filtering and antivirus are applied.
- Employee laptop computers can connect to the Internet, but web filtering is applied. They can also connect to company networks, but only if FortiClient Endpoint Security is installed to protect against viruses.

Figure 2 and Figure 3 show these policies implemented for WiFi to the company network and to the Internet.

Figure 2: Device policies for WiFi access to the company network

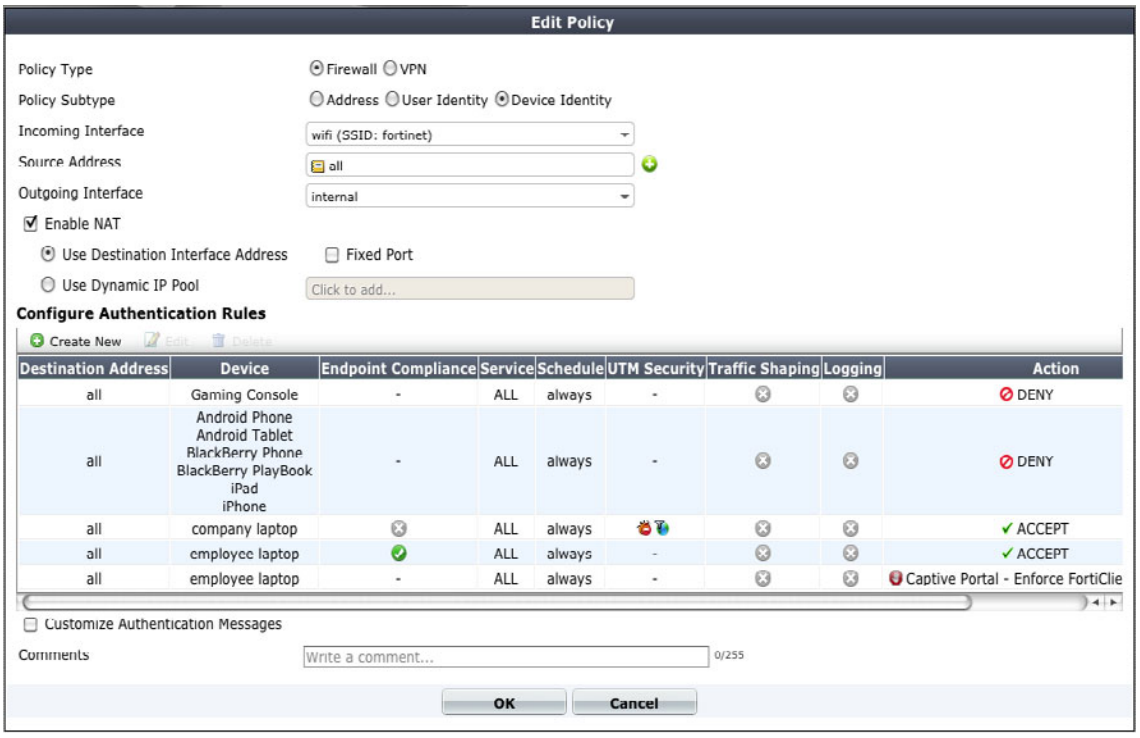
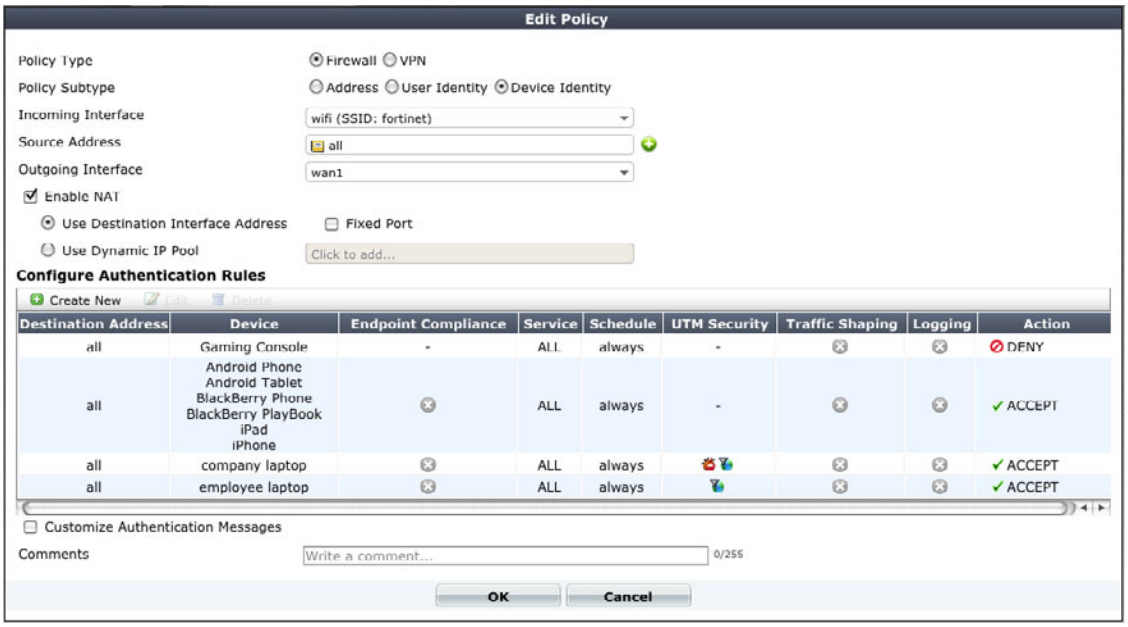


Figure 3: Device policies for WiFi access to the Internet



The next section explains device policy creation in detail.

Creating device policies

Device-based security policies are similar to policies based on user identity:

- The policy enables traffic to flow from one network interface to another.
- NAT can be enabled.
- Authentication rules can allow or deny specific devices or device groups.
- UTM protection can be applied.

To create a device identity policy

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. In *Policy Subtype*, select *Device Identity*.
3. Choose *Incoming Interface*, *Source Address*, and *Outgoing Interface* as you would for any security policy.
4. Select *Enable NAT* if appropriate.

   You are now ready to create authentication rules.

To create an authentication rule

1. Select *Create New.*
2. Enter *Destination*, *Schedule*, and *Service* as you would for any security policy.
3. In *Device*, select the devices or device groups to which this policy applies.

   You can select multiple devices or groups.
4. Select *Compliant with Endpoint Profile* if you want to enforce use of FortiClient Endpoint Security by the client devices. This is available here only if Action is ACCEPT. See "Adding endpoint control" next.
5. Select either ACCEPT or DENY as the policy Action.
6. Configure *UTM Security Profiles* as you would for any security policy.
7. Select *OK*.

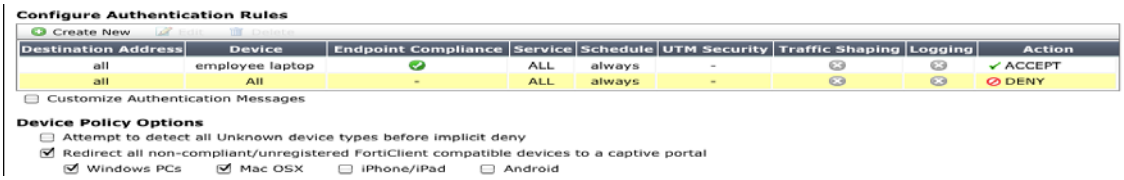
8. Select *OK* again to complete creation of the security policy.

Adding endpoint control

Optionally, you can require that users devices have FortiClient Endpoint Security software installed. The software provides FortiOS more detailed information about the applications being used. FortiOS pushes its endpoint profile to the FortiClient software, configuring network protection such as antivirus, application control, and web category filtering. Devices without an up-to-date installation of FortiClient software are restricted to a captive portal that provides links from which the user can download a FortiClient installer.

If you have already created an ACCEPT rule for particular device groups, you simply edit this rule and enable *Compliant with Endpoint Profile*. Then select the device policy option that directs FortiClient-compatible devices to a captive portal.

Figure 4: Endpoint compliance rule and captive portal rule



Setting Device Policy Options

1. Optionally, enable *Attempt to detect all Unknown device types before implicit deny*.
2. *Redirect all non-compliant/unregistered FortiClient compatible devices to a captive portal* enables a captive portal. Select which device platforms to include.
3. Optionally, enable *Prompt Email Address Collection Portal for all devices*. This requests an email address from the device user. See “Guest access in a retail environment” on page 66.

Example: access for employee devices

Employees can connect to the Internet and to your private corporate network with their mobile devices. To ensure that only employee devices can connect, you add employee devices to a custom device group and specify that group in the security policy.

Optionally, you can require employee devices to use FortiClient Endpoint Security software. The endpoint profile pushed out to the FortiClient software can require use of realtime antivirus protection and can impose restrictions on the applications that can be active while the device is attached to the network. See “Adding endpoint control” on page 14.

You need to

- Create a custom device group for employee devices.
- Create two device policies:
  - a policy that allows traffic to flow from the employee WiFi SSID to the Internet interface.
  - a policy that allows traffic to flow from the employee WiFi SSID to the private network interface.

Creating the employee custom device group

The predefined device groups are automatically populated. When you create a custom device group, you choose the members. Adding a device that the FortiGate unit has already detected is easiest. But you can also add a device that has not yet been detected if you know its MAC address.

To create the custom device group

1. Go to *User & Device* > *Device* > *Device Group* and select *Create New*.
2. Enter a name, Employees for example.
3. Select *OK*.

Creating the employee Internet access policy

To create a device identity policy for Internet access

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Enter the following information:

Policy Type	Firewall
Policy Subtype	Device Identity
Incoming Interface	byod-example
Source Address	all
Outgoing Interface	wan1
Enable NAT	Enable.

You are now ready to create the authentication rule.

To create the authentication rule

1. Select *Create New* again and enter:

Destination Address	all
Device	Employees
Compliant with Endpoint Profile	Not selected.
Schedule	Always
Service	All
Action	ACCEPT

2. Select *OK*.
3. Select *OK* to complete configuration of the security policy.

Creating the private network access policy

The policy to allow access to the private network is similar to the one for Internet access, except for the outgoing interface. The authentication rules that enforce FortiClient software use are identical.

To create a device identity policy for private network access

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Enter the following information:

Policy Type	Firewall
Policy Subtype	Device Identity
Incoming Interface	byod-example
Outgoing Interface	The interface that connects to the private network, port3 for example.
Enable NAT	Enable

3. Select *OK*.

   You are now ready to create the authentication rule.

To create the authentication rule

1. Select *Create New* again and enter:

Destination Address	all
Device	Employees
Compliant with Endpoint Profile	Not selected.
Schedule	Always
Service	All
Action	ACCEPT

2. Select *OK*.
3. Select *OK* to complete configuration of the security policy.

Adding endpoint control

You need to

- Configure the endpoint profile.
- Configure a device policy option to direct non-compliant endpoints that can run FortiClient software to a captive portal. Other devices will have network access as usual.

Configuring the endpoint profile

The endpoint profile determines the FortiClient configuration that will be pushed to devices.

To create an Endpoint profile

1. Go to *User & Device* > *Device* > *Endpoint Profile*.
2. Select the antivirus, application control, web filtering and so on that you require.
3. Select OK.

For information about antivirus, application control, web filtering, and vulnerability scanning, see the UTM chapter of the FortiOS Handbook.

Modifying the employee private network access policy

Go to *Policy* > *Policy* > *Policy* and open the private network access policy you created earlier.

To require FortiClient Endpoint Security use by PCs and MAC OSX computers

1. Open the authentication rule that you created before and select *Compliant with Endpoint Profile*. Then, select *OK*.
2. In *Device Policy Options*, select *Redirect all non-compliant/unregistered FortiClient compatible devices to a captive portal.*
3. Select *Windows PCs* and *Mac OSX*.
4. Select OK.

Customizing captive portals

Captive portals are defined in Replacement Messages that you can modify.

FortiClient download portal

This portal acts as a quarantine for devices that are not protected by FortiClient Endpoint Security. The portal provides links to obtain the FortiClient software. The user can retry connecting to the FortiGate unit after installing the FortiClient software.

Email address collection portal

This portal is used to collect an email address as a means of identifying the device user. When the email address has been verified, the device is added to the Collected Emails device group.

Table 2: Replacement messages that determine portal content

	Replacement Messages
FortiClient download	Endpoint NAC Feature Block Page
Email address collection	Email Collection Email Collection Invalid Email

To modify a portal

1. Open a device policy that uses the portal.
2. Select *Customize Authentication Messages*.
3. Select the *Edit* icon.
4. In *Messages*, select the replacement message to modify.
5. Edit the HTML code for the message and select *Save*.
6. Select *Close*.

Creating the WiFi SSID

Both guest and employee devices will need an SSID (WiFi network) with open security. This means that no passphrase is required to join the SSID. Device policies will determine who gets access to network resources. By default, open security is not available in the WiFi SSID configuration.

To make open WiFi authentication available - web-based manager

1. Go to *System* > *Admin* > *Settings*.
2. Under *Display Options on GUI*, enable *Wireless Open Security* and select *Apply*.

To make open WiFi authentication available - CLI

```
config system global
  set gui-wireless-opensecurity enable
end
```

To configure the SSID - web-based manager

1. Go to *WiFi Controller* > *WiFi Network* > *SSID* and select *Create New*.
2. Enter the following information and select OK:

Name	byod-example
IP/Netmask	10.10.110.1/24
Administrative Access	Ping (to assist with testing)
SSID	byod-guest
Enable DHCP	Enable
Address Range	10.10.110.2 - 10.10.110.199
Netmask	255.255.255.0
Default Gateway	Same As Interface IP
DNS Server	Same as System DNS
Security Mode	Open
Block Intra-SSID Traffic	Select.
Leave other settings at their default values.	

For detailed information about creating a WiFi SSID, see the Deploying Wireless Networks chapter of the FortiOS Handbook.

Configuring Internet access for guests with mobile devices

Guest devices have access only to the Internet. You need a device policy that allows traffic to flow from the WiFi SSID to the Internet interface. Within that policy, you need an authentication rules to allow access for the various types of devices.

To create the device policy

1. Go to *Policy* > *Policy* > *Policy* and select *Create New*.
2. Enter the following information:

Policy Type	Firewall
Policy Subtype	Device Identity
Incoming Interface	byod-example
Source Address	all
Outgoing Interface	wan1
Enable NAT	Enable.

You are now ready to create the authentication rule.

To create the authentication rule

1. In *Configure Authentication Rules*, select *Create New* and enter:

Destination Address	all
Device	Android Phone, Android Tablet, iPad, iPhone, Linux PC, Mac, Other Network Device, Windows PC
Compliant with Endpoint Profile	not selected
Schedule	always
Service	ALL
Action	ACCEPT

2. Select *OK*.
3. If asked, confirm that you accept FortiOS will enable device identification on the source interface.

   The rule is now configured.
4. Select *OK* to complete configuration of the security policy.

Endpoint Control

This section describes the Endpoint Control feature and how to configure it.

The following topics are included in this section:

Endpoint Control overview

Endpoint Control ensures that workstation computers (endpoints) meet security requirements, otherwise they are not permitted access. Endpoint Control enforces the use of FortiClient Endpoint Security and pushes a configuration to the FortiClient application that can specify any of the following:

- Real-time antivirus protection - on or off
- FortiClient application control (application firewall) using application sensors defined in the FortiGate application control feature
- FortiClient web category filtering based on web filters defined in a FortiGate web filter profile
- Endpoint vulnerability scanning daily, weekly, or monthly
- VPN configurations
- Uploading of logs to the FortiGate unit hourly or daily
- Configuration profile (.mobileconfig file for iOS)

Non-compliant endpoints are those without the latest version of FortiClient installed. They can be sent to the FortiClient download portal to obtain FortiClient software, or blocked.

Of the features listed above, enforcement of FortiClient licensing and FortiClient web content filtering can be configured only through the CLI using the `config endpoint-control profile` command.

Endpoint Control settings are grouped into one or more Endpoint Control profiles. You enable Endpoint Security in device identity firewall policies and select an Endpoint Control profile.

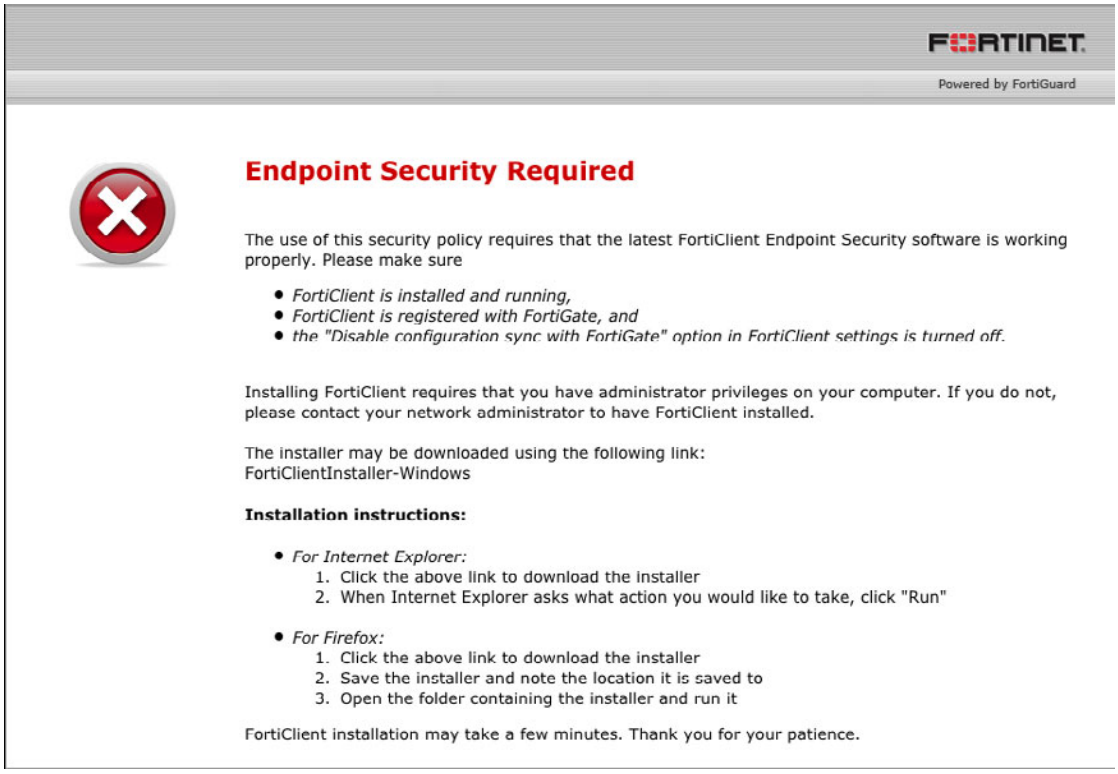
User experience

Endpoint Control applies to users attempting to make a connection that is controlled by a firewall policy that specifies an endpoint profile. The user of a non-compliant endpoint using a web browser receives a replacement message HTML page from the FortiGate unit. The message explains the non-compliance. Depending on the endpoint profile, the user may be allowed to continue or id blocked from further access. For information about modifying these replacement pages, see "Modifying the Endpoint Security replacement message" on page 25.

FortiClient non-compliance

If the authentication rule in a device identity policy specifies an endpoint profile, a device without the latest version of FortiClient Endpoint Security installed sees a message like this:

Figure 5: Default FortiClient non-compliance message



If there is a FortiClient installer available for the endpoint computer's operating system, a link is provided to download the installer. If there is no installer available, the user is asked to contact the network administrator.

After installing FortiClient Endpoint Security, the user will receive an invitation to register with the FortiGate unit. If the user accepts the invitation, the endpoint profile is sent to the device's FortiClient application. Now the user can pass the authentication rule and connect to the network. FortiClient Endpoint Security registered with a FortiGate unit does not need to be separately licensed with FortiGuard.

Registration for remote users

The FortiGate unit can also register endpoints who connect over the Internet through a VPN. The user can accept an invitation to register with the FortiGate unit. See "Configuring endpoint registration over a VPN" on page 24.

FortiGate endpoint registration limits

To view the number of endpoints that are registered and the total that can be registered, go to *System* > *Dashboard* > *Status*. Under *License Information*, find *FortiClient Software*. You will see a line like “Registered/Allowed 4 of 10”. This means that there are four registered endpoints and a total of ten are allowed. For all FortiGate models, the maximum number of registered endpoints is ten. For all models except 20C and 40C, you can purchase an endpoint license to increase this capacity:

Table 3: Maximum registered endpoints with endpoint license

	Max Registered Endpoints
Desktop	200
Rack - 1U	2000
Rack - 2U+	8000

When the registration limit is reached, the next FortiClient-compatible device will not be able to register with the FortiGate unit. The user sees a message in FortiClient application about this. The endpoint profile is not sent to client and the client cannot connect through the FortiGate unit.

To add an endpoint license - web-based manager

1. Go to *System* > *Dashboard* > *Status*.
2. Under FortiClient Software, select *[Enter License]*, enter the license key, and select *OK*.

Configuration overview

Endpoint Control requires that all hosts using the firewall policy have the FortiClient Endpoint Security application installed. Make sure that all hosts affected by this policy are able to install this application. Currently, FortiClient Endpoint Security is available for Microsoft Windows (2000 and later) and Apple Mac OSX only.

To set up Endpoint Control, you need to

- Enable Central Management by the FortiGuard Analysis & Management Service if you will use FortiGuard Services to update the FortiClient application or antivirus signatures. You do not need to enter account information. See “Centralized Management” in the System Administration chapter of the FortiOS Handbook.
- By default, the FortiGuard service provides the FortiClient installer. If you prefer to host it on your own server, see “Changing the FortiClient installer download location” on page 21.
- In UTM Security Profiles, configure application sensors and web filters profiles as needed to monitor or block applications. See the UTM Guide chapter of the FortiOS Handbook.for details.
- Create an endpoint control profile or use a predefined profile. See “Creating an endpoint profile” on page 21. Enable the application sensor and web category filtering profiles that you want to use.
- Enable Endpoint Security in firewall policies, selecting the appropriate endpoint control profile.
- Optionally, configure the FortiGate unit to support endpoint registration by IPsec or SSL VPN.

Changing the FortiClient installer download location

By default, FortiClient installers are downloaded from the FortiGuard network. You can also host these installers on a server for your users to download. In that case, you must configure FortiOS with this custom download location. For example, to set the download location to a customer web server with address custom.example.com, enter the following command:

```
config endpoint-control settings
  set download-location custom
  set download-custom-link "http://custom.example.com"
end
```

Creating an endpoint profile

When an endpoint profile is selected in a firewall policy, all users of that firewall policy must have FortiClient Endpoint Security installed. The FortiGate unit pushes the endpoint profile settings to the FortiClient application on the client.

To create an endpoint control profile - web-based manager

1. If you will use the Application Firewall feature, go to *UTM Security Profiles* > *Application Control* > *Application Sensor* to create the Application Sensors that you will need.
2. If you will use Web Category Filtering, go to *UTM Security Profiles* > *Web Filter* > *Profile* to create the web filter profile that you will need.
3. Go to *User & Device* > *Device* > *Endpoint Profile.*

   The default profile is selected. At the top right of the window, you can also:

   - view the list of endpoint profiles
   - create a new endpoint profile
   - select another existing endpoint profile
4. In *Assign to Device Groups*, select one or more device groups to which this endpoint profile applies. This is not available for the default profile.
5. Enter the *FortiClient Configuration Deployment* settings for *Windows and Mac*:

Antivirus Realtime Protection on Client	ON — enable the FortiClient realtime AV feature.
Application Firewall	ON — enable application control. Select the application sensor to use.
Web Category Filtering	ON — enable web category filtering. Select the web filter profile to use.
Disable Web Category Filtering when protected by this FortiGate	Disables FortiClient web category filtering when client traffic is filtered by the FortiGate unit. Selected by default.
Endpoint Vulnerability Scan on Client	ON — FortiGate unit will perform vulnerability scan on client. Select the desired schedule.
Initiate Scan After Client Registration	Enables scan following registration, regardless of schedule. Selected by default.

Client VPN Provisioning	Enable to configure the FortiClient VPN client. Enter the VPN configuration details.
Upload logs to FortiAnalyzer /FortiManager	ON — FortiClient software will upload its logs to the specified FQDN or IP address. Select the desired schedule. Optionally, you can enable *Failover to FDN when FortiManager is not available*.
Use FortiManager for client software/signature update	ON — FortiClient software obtain AV signatures and software updates from the specified FQDN or IP address.
Client UI Options	ON — Select which FortiClient features to make visible to the user on the device.

6. Select OK.
7. Enter the *FortiClient Configuration Deployment* settings for *iOS*:

Web Category Filtering	ON — enable web category filtering. Select the web filter profile to use.
Disable Web Category Filtering when protected by this FortiGate	Disables FortiClient web category filtering when client traffic is filtered by the FortiGate unit. Selected by default.
Client VPN Provisioning	Enable to configure the FortiClient VPN client. You can enter multiple VPN configurations by selecting the “+” button.
Profile Name	Enter a name to identify this VPN configuration in the FortiClient application.
Type	Select *IPsec* or *SSL-VPN*. If you select *IPsec*, select a *VPN Configuration File* that contains the required IPsec VPN configuration. The Apple iPhone Configuration Utility produces .mobileconfig files which contain configuration information for an iOS device. If you select *SSL-VPN*, enter the VPN configuration details.
Distribute Configuration Profile	ON — Distribute configuration information to iOS devices running FortiClient Endpoint Security. Select *Browse* and locate the file to be distributed. The Apple iPhone Configuration Utility produces .mobileconfig files which contain configuration information for an iOS device.

8. Select OK.

To create an endpoint control profile - CLI

This example creates a profile for Windows and Mac computers.

```
config endpoint-control profile
  edit ep-profile1
    set device-groups mac windows-pc
    config forticlient-winmac-settings
      set forticlient-av enable
      set forticlient-wf enable
      set forticlient-wf-profile default
    end
  end
```

Enabling Endpoint Control in firewall policies

Endpoint Control is applied to any traffic where the controlling firewall policy has Endpoint Security enabled. The device group to which the device belongs determines which Endpoint Control profile is applied. The policy searches the list of endpoint profiles starting from the top and applies the first profile assigned to the device group.

To enable Endpoint Control - web-based manager

1. Go to *Policy* > *Policy* > *Policy* and edit the device identity firewall policy where you want to enable Endpoint Control.
2. Create or edit an authentication rule.
3. Select *Compliant with Endpoint Profile*.
4. Select *OK*.

To configure the firewall policy - CLI

In this example, the LAN connects to Port 2 and the Internet is connected to Port 1. An Endpoint Control profile is applied.

```
config firewall policy
  edit 0
    set srcintf port2
    set dstintf port1
    set srcaddr LANusers
    set dstaddr all
    set action accept
    set identity-based enable
    set identity-from device
    set nat enable
    config identity-based-policy
      edit 1
        set schedule always
        set service ALL
        set devices all
        set endpoint-compliance enable
      end
  end
```

Configuring endpoint registration over a VPN

FortiGate units can register FortiClient-equipped endpoints over either an interface-based IPsec VPN or a tunnel-mode SSL VPN. After the user authenticates, the FortiGate unit sends the FortiClient application the IP address and port to be used for registration. If the user accepts the FortiGate invitation to register, registration proceeds and the endpoint profile is downloaded to the client.

Users without FortiClient Endpoint Security connecting to the SSL VPN through a browser can be redirected to a captive portal to download and install the FortiClient software. The security policy must enable *Redirect all non-compliant/unregistered FortiClient compatible devices to a captive portal*, but not select any specific device types.

Endpoint registration on an IPsec VPN

You can enable endpoint registration when you configure the FortiClient VPN or you can enable it on an existing FortiClient VPN.

To enable endpoint registration while configuring the VPN

- Enable *Endpoint Registration* on the *New FortiClient VPN* page.

To enable endpoint registration on an existing VPN

1. Go to *System* > *Network* > *Interface* and edit the VPN's tunnel interface.

   The tunnel is a subinterface of the physical network interface.
2. In *Administrative Access*, make sure that *FCT-Access* is enabled.
3. Select OK.

Endpoint registration on the SSL VPN

To enable endpoint registration on the SSL VPN

1. Go to *VPN* > *SSL* > *Portal.*
2. Make sure *Enable Tunnel Mode* is enabled.
3. Optionally, enable *Include FortiClient Download*.

   Users who access the VPN with a browser will be able to download FortiClient Endpoint Security for their device.
4. Select *Apply*.
5. Go to *VPN* > *SSL* > *Config*, make sure *Enable Endpoint Registration* is enabled, then select *Apply*.

This procedure does not include all settings needed to configure a working SSL VPN.

Synchronizing endpoint registrations

To support roaming users in a network with multiple FortiGate units, you need to configure synchronization of the endpoint registration databases between the units. The registered endpoints are then recognized on all of the FortiGate units. This is configured in the CLI. For example, to synchronize this FortiGate unit's registered endpoint database with another unit we call `other1` at IP address 172.20.120.4, enter:

```
config endpoint-control forticlient-registration-sync
  edit other1
    set peer-ip 172.20.120.4
  end
```

Modifying the Endpoint Security replacement message

The FortiGate unit sends an *Endpoint NAC Download Portal* page to a non-compliant endpoint that attempts to use a firewall policy in which Compliant with Endpoint Profile is enabled. There are different versions of this page for iOS, Mac, Windows, and other devices. Optionally, you can modify these pages.

To modify an Endpoint NAC Download Portal page

1. Go to *System* > *Admin* > *Settings* and ensure that the *Replacement Message Groups* display option is enabled.
2. Go to *System* > *Config* > *Replacement Message Group* and select *Create New*.
3. Enter a *Name* for the group.
4. In *Group Type*, select *Endpoint Control* and select *OK*.
5. Open the replacement message group that you just created and select the *Endpoint NAC Download Portal* message for the appropriate device type.

   The replacement message and its HTML code appear in a split screen in the lower half of the page.
6. Modify the text as needed and select *Save*.

Vulnerability Scan

The Network Vulnerability Scan helps you to protect your network assets (servers and workstations) by scanning them for security weaknesses. You can scan on-demand or on a scheduled basis. Results are viewable on the FortiGate unit, but results are also sent to an attached FortiAnalyzer unit. The FortiAnalyzer unit can collect the results of vulnerability scans from multiple FortiGate units at different locations on your network, compiling a comprehensive report about network security.

This section describes how to configure a single FortiGate unit for network scanning and how to view the results of the scan.

The following topics are included in this section:

Running and configuring scans and viewing scan results

You can configure regular network scans on a daily, weekly, or monthly basis.

To run a vulnerability scan

1. Go to *User & Device* > *Vulnerability Scan* > *Scan Definition* and select *Start Scan*.

   The vulnerability starts a scan using the current scanner settings. When the scan is running you can pause or stop it at any time. You can also watch the progress of the scan.
2. When the scan is complete go to *User & Device* > *Vulnerability Scan* > *Vulnerability Result* to view the results of the scan.

To configure scanning - web-based manager

1. Go to *User & Device* > *Vulnerability Scan* > *Scan Definition*.
2. Beside *Schedule* select *Change* to set the scan schedule and mode:

Recurrence	Select *Daily*, *Weekly*, or *Monthly* and configure the details for the option you have selected.
Suspend Scan between	Set a time during which the scan should be paused if its running.
Vulnerability Scan Mode	**Quick** — check only the most commonly used ports **Standard** — check the ports used by most known applications **Full** — check all TCP and UDP ports For a detailed list of the TCP and UDP ports examined by each scan mode, see Table 4 on page 31.

3. Select *Apply* to save the schedule and scan type.

4. Select *Create New* under *Asset Definitions* to select the devices on the network to scan.

   An asset can be a single server or workstation computer on your network or a range of addresses on your network. You must add assets to the vulnerability scan before you can run a scan.

   To scan an entire network or part of a network you can just add the appropriate IP address range to the asset configuration. You can also add the IP addresses of Windows and Linux computers to include the user names and passwords for these machines. The vulnerability scanner will use these credentials to log into the computers and do more detailed vulnerability scanning.

   Even if the asset is an address range you can add Windows and Linux credentials. The vulnerability scanner will attempt to log into all network device it finds using these credentials.

5. Enter the following information and select *OK*:

Name	Enter a name for this asset.
Type	Select *IP Address* to add a single IP address. Select *Range* to add a range of IP addresses to scan.
IP Address	Enter the IP address of the asset. (*Type* is *IP Address*.)
Range	Enter the start and end of the IP address range. (*Type* is *Range*.)
Enable Scheduled Vulnerability Scanning	Select to allow this asset to be scanned according to the schedule. Otherwise the asset is not scanned during a scheduled vulnerability scan.
Windows Authentication	Select to use authentication on a Windows operating system. Enter the username and password in the fields provided. For more information, see “Requirements for authenticated scanning and ports scanned” on page 28.
Unix Authentication	Select to use authentication on a Unix operating system. Enter the username and password in the fields provided. For more information, see “Requirements for authenticated scanning and ports scanned” on page 28.

6. Select *Apply* to save the configuration.

To add an asset - CLI

This example adds a single computer to the Asset list:

```
config netscan assets
  edit 0
    set name "server1"
    set addr-type ip
    set start-ip 10.11.101.20
    set auth-windows enable
    set win-username admin
    set win-password zxcvbnm
    set scheduled enable
  end
```

This example adds an address range to the Asset list. Authentication is not used:

```
config netscan assets
  edit 0
    set name "fileservers"
    set addr-type range
    set start-ip 10.11.101.160
    set end-ip 10.11.101.170
    set scheduled enable
  end
```

To configure scanning - CLI

To configure, for example, a standard scan to be performed every Sunday at 2:00am, you would enter:

```
config netscan settings
  set scan-mode standard
  set schedule enable
  set time 02:00
  set recurrence weekly
  set day-of-week sunday
end
```

To view vulnerability scan results

1. To view vulnerability scan results go to *User & Device* > *Vulnerability Scan* > *Vulnerability Result*.

Select any log entry to view log details.

Requirements for authenticated scanning and ports scanned

The effectiveness of an authenticated scan is determined by the level of access the FortiGate unit obtains to the host operating system. Rather than use the system administrator's account, it might be more convenient to set up a separate account for the exclusive use of the vulnerability scanner with a password that does not change.

Microsoft Windows hosts - domain scanning

The user account provided for authentication must

- have administrator rights
- be a Security type of account
- have global scope
- belong to the Domain Administrators group
- meet the Group Policy requirements listed below:

Group Policy - Security Options

In the Group Policy Management Editor, go to Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options.

Setting	Value
Network access: Sharing and security model for local accounts	Classic
Accounts: Guest account status	Disabled
Network access: Let Everyone permissions apply to anonymous users	Disabled

Group Policy - System Services

In the Group Policy Management Editor, go to Computer Configuration > Windows Settings > Security Settings > System Services.

Setting	Value
Remote registry	Automatic
Server	Automatic
Windows Firewall	Automatic

Group Policy - Administrative Templates

In the Group Policy Management Editor, go to Computer Configuration > Administrative Templates > Network > Network Connections > Windows Firewall > Domain Profile.

Setting	Value
Windows Firewall: Protect all network connections	Disabled

or

Setting	Value
Windows Firewall: Protect all network connections	Enabled
Windows Firewall: Allow remote administration exception	Enabled
Allow unsolicited messages from[1]	*
Windows Firewall: Allow file and printer sharing exception	Enabled
Allow unsolicited messages from[1]	*
Windows Firewall: Allow ICMP exceptions	Enabled
Allow unsolicited messages from[1]	*

[1]Windows prompts you for a range of IP addresses. Enter either "*" or the IP address of the Fortinet appliance that is performing the vulnerability scan.

Microsoft Windows hosts - local (non-domain) scanning

The user account provided for authentication must

- be a local account
- belong to the Administrators group

The host must also meet the following requirements:

- Server service must be enabled. (Windows 2000, 2003, XP)
- Remote Registry Service must be enabled.
- File Sharing must be enabled.
- Public folder sharing must be disabled. (Windows 7)
- Simple File Sharing (SFS) must be disabled. (Windows XP)

Windows firewall settings

- Enable the *Remote Administration Exception* in Windows Firewall. (Windows 2003, Windows XP)
- Allow *File and Print sharing* and *Remote Administration* traffic to pass through the firewall. Specify the IP address or subnet of the Fortinet appliance that is performing the vulnerability scan. (Windows Vista, 2008)
- For each of the active *Inbound Rules* in the *File and Printer Sharing* group, set the *Remote IP address* under *Scope* to either *Any IP address* or to the IP address or subnet of the Fortinet appliance that is performing the vulnerability scan. (Windows 7)

Unix hosts

The user account provided for authentication must be able at a minimum to execute these commands:

- The account must be able to execute “uname” in order to detect the platform for packages.
- If the target is running Red Hat, the account must be able to read /etc/redhat-release and execute “rpm”.
- If the target is running Debian, the account must be able to read /etc/debian-version and execute “dpkg”.

Table 4: Ports scanned in each scan mode

Scan Type	Ports scanned
Standard Scan	***TCP:*** 1-3, 5, 7, 9, 11, 13, 15, 17-25, 27, 29, 31, 33, 35, 37-39, 41-223, 242-246, 256-265, 280-282, 309, 311, 318, 322-325, 344-351, 363, 369-581, 587, 592-593, 598, 600, 606-620, 624, 627, 631, 633-637, 666-674, 700, 704-705, 707, 709-711, 729-731, 740-742, 744, 747-754, 758-765, 767, 769-777, 780-783, 786, 799-801, 860, 873, 886-888, 900-901, 911, 950, 954-955, 990-993, 995-1001, 1008, 1010-1011, 1015, 1023-1100, 1109-1112, 1114, 1123, 1155, 1167, 1170, 1207, 1212, 1214, 1220-1222, 1234-1236, 1241, 1243, 1245, 1248, 1269, 131t3-1314, 1337, 1344-1625, 1636-1774, 1776-1815, 1818-1824, 1901-1909, 1911-1920, 1944-1951, 1973, 1981, 1985-2028, 2030, 2032-2036, 2038, 2040-2049, 2053, 2065, 2067, 2080, 2097, 2100, 2102-2107, 2109, 2111, 2115, 2120, 2140, 2160-2161, 2201-2202, 2213, 2221-2223, 2232-2239, 2241, 2260, 2279-2288, 2297, 2301, 2307, 2334, 2339, 2345, 2381, 2389, 2391, 2393-2394, 2399, 2401, 2433, 2447, 2500-2501, 2532, 2544, 2564-2565, 2583, 2592, 2600-2605, 2626-2627, 2638-2639, 2690, 2700, 2716, 2766, 2784-2789, 2801, 2908-2912, 2953-2954, 2998, 3000-3002, 3006-3007, 3010-3011, 3020, 3047-3049, 3080, 3127-3128, 3141-3145, 3180-3181, 3205, 3232, 3260, 3264, 3267-3269, 3279, 3306, 3322-3325, 3333, 3340, 3351-3352, 3355, 3372, 3389, 3421, 3454-3457, 3689-3690, 3700, 3791, 3900, 3984-3986, 4000-4002, 4008-4009, 4080, 4092, 4100, 4103, 4105, 4107, 4132-4134, 4144, 4242, 4321, 4333, 4343, 4443-4454, 4500-4501, 4567, 4590, 4626, 4651, 4660-4663, 4672, 4899, 4903, 4950, 5000-5005, 5009-5011, 5020-5021, 5031, 5050, 5053, 5080, 5100-5101, 5145, 5150, 5190-5193, 5222, 5236, 5300-5305, 5321, 5400-5402, 5432, 5510, 5520-5521, 5530, 5540, 5550, 5554-5558, 5569, 5599-5601, 5631-5632, 5634, 5678-5679, 5713-5717, 5729, 5742, 5745, 5755, 5757, 5766-5767, 5800-5802, 5900-5902, 5977-5979, 5997-6053, 6080, 6103, 6110-6112, 6123, 6129, 6141-6149, 6253, 6346, 6387, 6389, 6400, 6455-6456, 6499-6500, 6515, 6558, 6588, 6660-6670, 6672-6673, 6699, 6767, 6771, 6776, 6831, 6883, 6912, 6939, 6969-6970, 7000-7021, 7070, 7080, 7099-7100, 7121, 7161, 7174, 7200-7201, 7300-7301, 7306-7308, 7395, 7426-7431, 7491, 7511, 7777-7778, 7781, 7789, 7895, 7938, 7999-8020, 8023, 8032, 8039, 8080-8082, 8090, 8100, 8181, 8192, 8200, 8383, 8403, 8443, 8450, 8484, 8732, 8765, 8886-8894, 8910, 9000-9001, 9005, 9043, 9080, 9090, 9098-9100, 9400, 9443, 9535, 9872-9876, 9878, 9889, 9989-10000, 10005, 10007, 10080-10082, 10101, 10520, 10607, 10666, 11000, 11004, 11223, 12076, 12223, 12345-12346, 12361-12362, 12456, 12468-12469, 12631, 12701, 12753, 13000, 13333, 14237-14238, 15858, 16384, 16660, 16959, 16969, 17007, 17300, 18000, 18181-18186, 18190-18192, 18194, 18209-18210, 18231-18232, 18264, 19541, 20000-20001, 20011, 20034, 20200, 20203, 20331, 21544, 21554, 21845-21849, 22222, 22273, 22289, 22305, 22321, 22555, 22800, 22951, 23456, 23476-23477, 25000-25009, 25252, 25793, 25867, 26000, 26208, 26274, 27000-27009, 27374, 27665, 29369, 29891, 30029, 30100-30102, 30129, 30303, 30999, 31336-31337, 31339, 31554, 31666, 31785, 31787-31788, 32000, 32768-32790, 33333, 33567-33568, 33911, 34324, 37651, 40412, 40421-40423, 42424, 44337, 47557, 47806, 47808, 49400, 50505, 50766, 51102, 51107, 51112, 53001, 54321, 57341, 60008, 61439, 61466, 65000, 65301, 65512 ***UDP:*** 7, 9, 13, 17, 19, 21, 37, 53, 67-69, 98, 111, 121, 123, 135, 137-138, 161, 177, 371, 389, 407, 445, 456, 464, 500, 512, 514, 517-518, 520, 555, 635, 666, 858, 1001, 1010-1011, 1015, 1024-1049, 1051-1055, 1170, 1243, 1245, 1434, 1492, 1600, 1604, 1645, 1701, 1807, 1812, 1900, 1978, 1981, 1999, 2001-2002, 2023, 2049, 2115, 2140, 2801, 3024, 3129, 3150, 3283, 3527, 3700, 3801, 4000, 4092, 4156, 4569, 4590, 4781, 5000-5001, 5036, 5060, 5321, 5400-5402, 5503, 5569, 5632, 5742, 6073, 6502, 6670, 6771, 6912, 6969, 7000, 7300-7301, 7306-7308, 7778, 7789, 7938, 9872-9875, 9989, 10067, 10167, 11000, 11223, 12223, 12345-12346, 12361-12362, 15253, 15345, 16969, 20001, 20034, 21544, 22222, 23456, 26274, 27444, 30029, 31335, 31337-31339, 31666, 31785, 31789, 31791-31792, 32771, 33333, 34324, 40412, 40421-40423, 40426, 47262, 50505, 50766, 51100-51101, 51109, 53001, 61466, 65000

Table 4: Ports scanned in each scan mode

Scan Type	Ports scanned
Full Scan	All TCP and UDP ports (1-65535)
Quick Scan	***TCP:*** 11, 13, 15, 17, 19-23, 25, 37, 42, 53, 66, 69-70, 79-81, 88, 98, 109-111, 113, 118-119, 123, 135, 139, 143, 220, 256-259, 264, 371, 389, 411, 443, 445, 464-465, 512-515, 523-524, 540, 548, 554, 563, 580, 593, 636, 749-751, 873, 900-901, 990, 992-993, 995, 1080, 1114, 1214, 1234, 1352, 1433, 1494, 1508, 1521, 1720, 1723, 1755, 1801, 2000-2001, 2003, 2049, 2301, 2401, 2447, 2690, 2766, 3128, 3268-3269, 3306, 3372, 3389, 4100, 4443-4444, 4661-4662, 5000, 5432, 5555-5556, 5631-5632, 5634, 5800-5802, 5900-5901, 6000, 6112, 6346, 6387, 6666-6667, 6699, 7007, 7100, 7161, 7777-7778, 8000-8001, 8010, 8080-8081, 8100, 8888, 8910, 9100, 10000, 12345-12346, 20034, 21554, 32000, 32768-32790 ***UDP:*** 7, 13, 17, 19, 37, 53, 67-69, 111, 123, 135, 137, 161, 177, 407, 464, 500, 517-518, 520, 1434, 1645, 1701, 1812, 2049, 3527, 4569, 4665, 5036, 5060, 5632, 6502, 7778, 15345

Client Reputation

The UTM scan types available on FortiGate units are varied and tailored to detect specific attacks. Sometimes however, user/client behavior can increase the risk of attack or infection. For example, if one of your network clients receives email viruses on a daily basis while no other clients receive these attachments, extra measures may be required to protect the client, or a discussion with the user about this issue may be worthwhile. Before you can decide on a course of action however, you need to know the problem is occurring. Client reputation can provide this information by tracking client behavior and reporting on the activities you determine are risky or otherwise noteworthy.

Client reputation only highlights risky activity and does not include tools to stop it. Instead, client reputation is a tool that exposes risky behavior. When you uncover risky behavior that you are concerned about you can take additional action to stop it. That action could include adding more restrictive security policies to block the activity or increase UTM protection.

Activities you can track include:

- Bad Connection Attempts: Typical BOT behavior is to connect to some hosts that do not exist on the Internet. This is because the BOT home needs to constantly change itself to dodge legislative enforcement, or just to hide from AV vendors. Bad connection attempts are tracked by:
  - Look ups for a DNS name that does not exist.
  - Connection attempts to an IP address that has no route.
  - HTTP 404 errors
- Packets that are blocked by deny security policies.
- Intrusion protection: Attack detected. Effect on reputation increases with severity of attack. Requires a subscription to FortiGuard IPS updates.
- Malware protection: Malware detected. Requires a subscription to FortiGuard Antivirus updates.
- Web activity: Visit to web site in risky categories, including Potentially Liable, Adult/Mature Content, Bandwidth Consuming, and Security Risk. Requires a subscription to FortiGuard Web Filtering.
- Application protection: Client uses software in risky categories, including Botnet, P2P, Proxy, and Games applications. Requires a subscription to FortiGuard IPS updates.
- Geographical locations that clients are communicating with. Requires access to the FortiGuard geographic database and a valid Fortinet support contract.

From among the activities you can track, you can configure how severely each activity will impact the reputation of the client in a sliding scale of Low, Medium, High, or Critical. If choose to ignore an activity, you can set it to Off, and it will have no affect on reputation.

You can turn on client reputation tracking for your FortiGate unit by going to *User & Device* > *Client Reputation* > *Reputation Definition*. Turning on client reputation tracking turns on logging for all security policies and all traffic accepted by security policies is tracked by client reputation. While client reputation is enabled logging cannot be turned off for these policies.

To support client reputation your FortiGate unit must be registered, have a valid support contract, and be licensed for FortiGuard antivirus, IPS, and Web Filtering. Your FortiGate unit must also be able to record log messages. Most FortiGate units can record log messages onto an internal log disk and can display client reputation results on the Client Reputation Monitor (go to *User & Device* > *Client Reputation* > *Reputation Score*). If your FortiGate unit does not record log messages onto an internal log disk, you can record client reputation data on a FortiAnalyzer unit and view the results from the FortiAnalyzer client reputation report.

After client reputation is turned on, the FortiGate unit tracks recent behavior using a sliding window and displays current data for this window. The default window size is 7 days, so the client reputation monitor represents behavior for the last 7 days (or since the service was started). The client reputation monitor displays clients and their activities in charts ordered according to how risky the behavior exhibited by the client is.

Data displayed by the client reputation monitor is extracted from the logging database. Data older than the window size is purged from the database.

Enabling client reputation adds a small amount of data to the logging database and can affect system performance if you had not been using traffic logging.

This chapter describes:

Applying client reputation monitoring to your network

You apply client reputation monitoring to network traffic by going to *User & Device* > *Client Reputation* > *Reputation Definition* turning on *Client Reputation Tracking* and selecting *Apply*.

Then you can optionally change the client reputation profile used by your FortiGate unit or you can accept the default profile. The client reputation profile indicates how risky you consider different types of client behavior to be. See “Setting the client reputation profile/definition” on page 36 for details.

Viewing client reputation results

After client reputation is enabled it takes a period of time to establish baseline network activity. The default time for this baseline, called the reporting window, to be established is 7 days. (To change it, see “Client reputation data update and maintenance intervals” on page 36).

The client reputation monitor is only visible if your FortiGate unit can save log messages to its internal hard disk. You can also send log messages to a FortiAnalyzer unit and use the FortiAnalyzer client reputation report to view client reputation data.

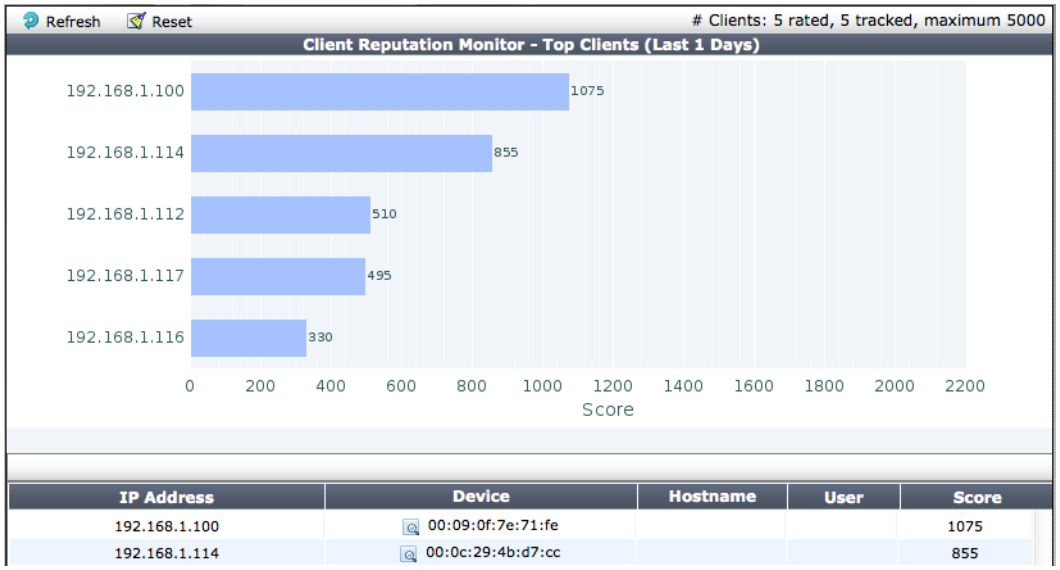
After the reporting window period, the FortiGate unit begins displaying client reputation results. To view the results go to *User & Device* > *Client Reputation* > *Reputation Score* to view the client reputation monitor. The monitor displays information about risky behavior as it was found. You can drill down into individual items to get more information about the behavior found and the client that caused it.

The client reputation monitor updates every 2 minutes. You can also select *Refresh* to manually update the display.

Select *Reset* to clear all client reputation data and restart the reporting window.

Figure 6 shows example client reputation results that shows activity from for different IP addresses that matched the kinds of traffic to be monitored according to the client reputation profile. You can see the IP address or name of each client and the amount of risky activity detected. The list at the bottom of the display shows more information about each device. The device information is gathered from enabling device monitoring by going to *User & Device* > *Device* > *Device Definition*.

Figure 6: Example client reputation results



You can select any of the bars in the graph to view information for each time the risky behavior was detected during the past 7 days (or whatever the Client Reputation window is). Information for each event detected includes the date and time the event was detected, the destination address, the application, and the client reputation score.

Changing the client reputation reporting window

By default, client reputation reports on activity for the last seven days. You can change this reporting window using the following command:

```
config client-reputation profile
  set window-size <interval_int>
end
```

Where <interval-int> is the reporting window in days. Range 1 to 30 days, default 7 days.

Client reputation data update and maintenance intervals

Client reputation updates its database every 2 minutes by querying the log database for client reputation information. This means that data displayed in the client reputation monitor is very current, at the most 2 minutes old.

Client reputation includes a data maintenance routine that runs every 12 hours to perform maintenance functions on the client reputation database. This routine:

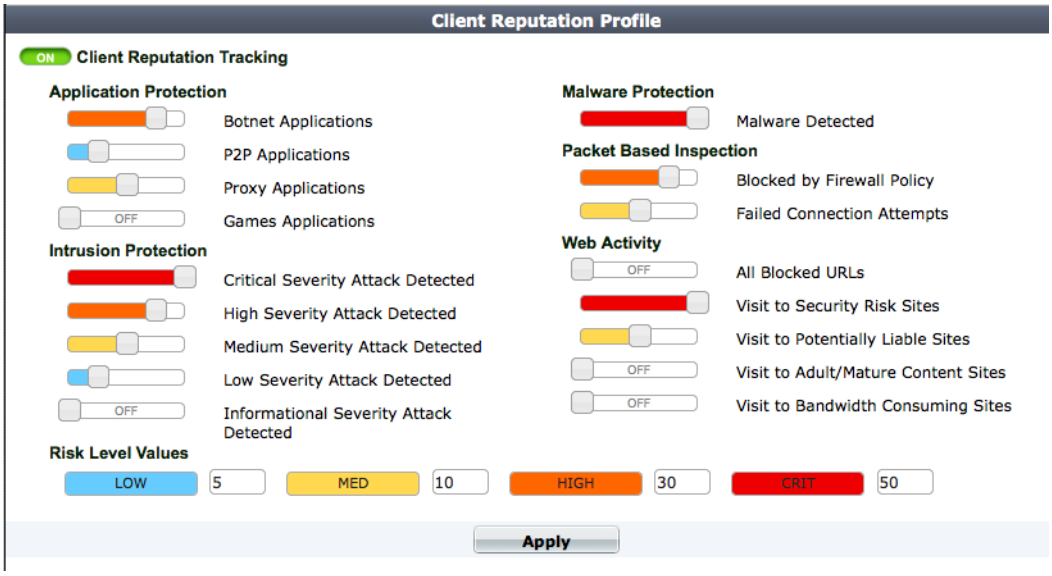
- Checks the number of tracked hosts. If the number is at the maximum of 5000, the maintenance routing removes the oldest ten percent (500) of hosts from the list. If the number is less than the maximum, nothing changes.
- Deletes any reputation data associated with a host that is not in the tracking list (usually this only occurs if hosts are removed).
- Deletes any reputation data that is older than the current time minus the window-size in days.

Setting the client reputation profile/definition

Configure the client reputation profile by going to *User & Device* > *Client Reputation* > *Reputation Definition*. You configure one client reputation profile for all of the activity monitored by the FortiGate unit. The profile sets the risk levels for the types of behavior that client reputation monitors. You can set the risk to off, low, medium, high and critical for the following types of behavior:

- Application Protection
  - Botnet applications
  - P2P applications
  - Proxy applications
  - Games applications
- Intrusion protection (IPS)
  - Critical severity attack detected
  - High severity attack detected
  - Medium severity attack detected
  - Low severity attack detected
  - Informational severity attack detected
- Malware Protection
  - Malware detected
- Packet based inspection
  - Packets blocked by firewall policy
  - Failed connection attempts
- Web Activity
  - All blocked URLs
  - Visit to security risk sites
  - Visit to potentially liable sites
  - Visit to adult/mature content sites
  - Visit to bandwidth consuming sites

Figure 7: Default client reputation profile



To configure the profile, decide how risky or dangerous each of the types of behavior are to your network and rate them accordingly. The higher you rate a type of behavior the more visible clients engaging in this behavior will become in the client reputation monitor and the more easily you can detect this behavior.

For example, if you consider malware a high risk for your network you can set the client reputation profile for malware to high or critical (as it is in the default client reputation profile). Then, whenever any amount of malware is detected, clients that originated the malware will be very visible in the client reputation monitor.

Set the risk to off for types of activity that you do not want client reputation to report on. This does not reduce the performance requirements or the amount of data gathered by client reputation, just the report output.

You can change a profile setting at any time and data that has already been collected will be used.

You can also change the *Risk Level Values*. Normally you would not need to change these settings, but you can change them if you want to alter the relative importance of the risk settings.

Expanding client reputation to include more types of behavior

You can use the following command to change the client reputation profile from the CLI to include client reputation reporting about more settings:

```
config client-reputation profile
```

In addition to the settings configurable from the web-based manager you can also set the following options:

- `geolocation-status` to enable or disable reporting on connections to and from different countries (geographical locations). For example, use the following command to indicate that you consider communication with Aruba to be medium risk:

```
config client-reputation profile
  set geolocation-status enable
    config geolocation
      edit 0
        set country AW
        set level medium
      end
  end
```

- `url-block-detected-status` to enable or disable reporting on connections blocked by web filtering. Use the following command to enable reporting about blocked URLs and set the risk level to medium:

```
config client-reputation profile
  set url-block-detected-status enable
  set url-block-detected-level medium
end
```

From the CLI you can configure client reputation to report more FortiGuard web filtering categories and more types of applications. For example, to report on social network activity (application control category 23):

```
config client-reputation-profile
  config application
    edit 0
      set category 23
      set level medium
    end
  end
```

To report on the local web filtering category (category 22):

```
config client-reputation-profile
  config web
    edit 0
      set group 22
      set level medium
    end
  end
```

Client reputation execute commands

The `execute client-reputation` command includes the following options:

- `add-host`, adds a host to client reputation tracking,
- `delete-host`, deletes a host from client reputation tracking,
- `display`, displays client reputation data for a host,
- `erase`, erases all client reputation data,
- `get-host-count`, displays the number of hosts monitored by client reputation.
- `get-timestamps`, displays client reputation related timestamps.
- `purge`, purges old client reputation data.
- `update`, updates client reputation data.

Client reputation diagnose commands

The `diagnose client-reputation` command includes the following options

- `convert-timestamp` convert a client reputation database timestamp to date and time
- `test-all` adds log messages from multiple sources to the client reputation database for testing
- `test-app` adds application control log messages to the client reputation database for testing
- `test-ips` adds Intrusion Protection log messages to the client reputation database for testing
- `test-webfilter` adds webfilter log messages to the client reputation database for testing

Index